



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Richmond Division

IN THE MATTER OF THE SEARCH OF
DISCLOSURE OF STORED
TELECOMMUNICATION RECORDS ON
CALL NUMBER **(804) 433-8241**, WITH
IMEI **357341090891638**,
THAT IS STORED AT PREMISES
CONTROLLED BY **T-Mobile**.

Case No. 3:21sw 141

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Leary, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) for information associated with a cellular telephone assigned call number **(804) 433-8241**, with International Mobile Equipment Identity (IMEI) **357341090891638** (“**SUBJECT ACCOUNT**”), that is serviced by **T-Mobile**, a wireless telephone service provider headquartered at **3625 132nd Ave SE, Bellevue, WA 98006**. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require **T-Mobile** to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate items described in Section II of Attachment B.

2. Your affiant is a law enforcement officer within the meaning of Title 18, United States Code, Section 2510(7), that is an officer of the United States who is empowered by law to

conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516. I am a Special Agent with the Richmond, Virginia, office of the Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) and have been employed as a Special Agent since July 2003. I am currently a member of the Richmond Division Child Exploitation Task Force and have been since March 2018. I have participated in investigations involving sexual assaults, persons who produce, collect, and distribute child pornography, and the importation and distribution of materials relating to the sexual exploitation of children. I have received training in the areas of sexual assaults and child exploitation, and I have reviewed images and videos of child pornography in a wide variety of media forms, including computer media. I have also discussed and reviewed these materials with other law enforcement officers. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of Title 18, United States Code, Sections 2252 and 2252A involving child exploitation offenses.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252A(a)(2)(A), that is, receipt of child pornography, have been committed by DEON RICHARD DOUGLAS and evidence thereof can be located in the

SUBJECT ACCOUNT. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes as further described in Attachment B.

5. The Court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. HSI is conducting a criminal investigation involving the receipt of child pornography and criminal violations including, among others, receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2)(A). DEON RICHARD DOUGLAS (“DOUGLAS”) is the subject of this investigation, and it is believed that from on or about April 15, 2020 through approximately November 14, 2020, DOUGLAS received pictures and videos constituting child pornography from a female victim identified to be sixteen years old when the media was received by DOUGLAS.

7. On December 20, 2020, DOUGLAS was driving in San Fernando, California when local police conducted a traffic stop of the vehicle DOUGLAS operated related to a registration violation. In the vehicle with DOUGLAS was the minor victim (“V1”) who was 17 years-old at the time, and her 15-year-old brother. Law enforcement inquired about the relationship between DOUGLAS and the minors in the vehicle. They were ultimately able to determine that DOUGLAS was in a relationship with V1. DOUGLAS stated that he had recently moved to California and lived in Virginia prior to his move. DOUGLAS granted Officers consent to search his vehicle and his cellular telephone, assigned call number **(804) 433-8241**.

DOUGLAS granted Officers consent to search the cellular telephone. Officers observed naked images of V1 on DOUGLAS's cellular telephone. DOUGLAS was arrested for possession of child pornography.

8. On December 22, 2020, V1 was forensically interviewed. During the interview, V1 revealed that DOUGLAS knew V1 was under the age of 18 and that he sent her pictures of his penis. V1 confirmed that V1 sent DOUGLAS sexually explicit pictures of herself. According to V1, DOUGLAS and V1 met online when she was around thirteen of fourteen years old. DOUGLAS and V1 mainly communicated over Instagram and their Instagram accounts were provided.

9. On December 23, 2020, HSI Northridge obtained a federal search warrant for DOUGLAS's cellular telephone and the Instagram accounts associated with DOUGLAS and V1. An analysis of DOUGLAS's cellular telephone conducted by HSI Northridge found it contained 105 images and 10 videos of child sexual abuse material (CSAM). CSAM refers to any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. DOUGLAS's cellular telephone also contained 86 images and two videos of child exploitative material (CEM) that refers to any representation of a child meant to exploit for sexual purposes which does not necessarily meet the federal definition of child pornography.

10. I observed one of these videos that was saved to DOUGLAS's cellular telephone. This video depicted an Instagram video call that occurred between DOUGLAS and V1 on or about July 13, 2020, when V1 was 16 years old. DOUGLAS' picture is displayed on the top half of the screen and the victim's picture is on the bottom half. The video is 10 minutes and 10 seconds long. Throughout the call, V1 is laying on a bed while wearing a shirt without pants or

underwear. V1 is holding the camera in a way that displays her buttocks and vagina.

DOUGLAS appears to watch V1 display her genitalia as he is seen touching his penis.

DOUGLAS is watching the video while listening with headphones and uses the chat function to type, "Spread the cheeks". V1 complies with his request to give him a better view of her vagina.

V1 continues to display her buttocks and vagina for DOUGLAS while he appears to masturbate.

Once he is finished, V1 turns off her camera.

11. I reviewed the download of Douglas's cellular telephone and found that it had used two phone numbers. Most recently a California area code number 818-941-3199, and previously a Virginia area code number 804-433-8241.

12. On June 23, 2021, I provided T-Mobile with a summons for phone number 804-433-8241, the SUBJECT ACCOUNT, used by DOUGLAS's cellular telephone. T-Mobile later replied that the 804-433-8241 account was in the name of DEON DOUGLAS at 718 W Clay St, Richmond, VA 23220. The SUBJECT ACCOUNT was established on August 11, 2017 and was still active as of December 21, 2020.

13. From the T-Mobile Summons, I found that DOUGLAS began utilizing his iPhone with Electronic Serial Number (ESN) 357341090891638 on or about April 13, 2020. I compared this date with the downloaded information obtained from the search warrant of the iPhone and found that the iPhone was used beginning on or about April 15, 2020. On or about April 15, 2020, a series of pictures that had been previously taken was transferred onto the new iPhone. Some of these transferred pictures contained CSAM images of V1 who was identified to be sixteen years old on April 15, 2020. DOUGLAS' iPhone assigned ESN 357341090891638 was used by DOUGLAS between April 15, 2020 and the date it was seized on December 20, 2020.

During this time, DOUGLAS transferred pictures of V1 onto the device and then continued to utilize it to receive and record images of V1 that constitute child pornography.

14. A Virginia Employment Commission (VEC) Wage Report for DOUGLAS reported that he had earnings in all four quarters of 2020 in Virginia.

15. The Driver's License DOUGLAS provided to the police during the December 20, 2020 traffic stop provided his home address as 718 W Clay St, Richmond, VA 23220.

16. In my training and experience, I have learned that **T-MOBILE** is a company that provides cellular telephone access to the general public. I also know that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

17. Based on my training and experience, I know that **T-MOBILE** can collect cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes. In my training and experience, this information may constitute evidence of the crimes under investigation

because the information can identify the location, patterns of movements and interstate travel taken by DOUGLAS while using the SUBJECT ACCOUNT. According to an email received from T-Mobile law enforcement relations unit, “historical cell site location information is stored for approximately 24 months following usage.”

18. Based on my training and experience, I know that wireless providers such as **T-MOBILE** typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service. I also know that wireless providers such as **T-MOBILE** typically collect and retain information about their subscribers’ use of the wireless service, such as records about calls or other communications sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the location of the call number **(804) 433-8241** and associated cellular device when the user he received the child pornography and interacted with V1 using his cellular data plan.

AUTHORIZATION REQUEST

19. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

20. I further request that the Court direct **T-Mobile** to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on **T-Mobile**, who will then compile the

requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Daniel Leary
Special Agent
Homeland Security Investigation

Subscribed and sworn to before me on September 20, 2021
at Richmond, Virginia.


/s/

Elizabeth W. Hanes
United States Magistrate Judge

ATTACHMENT A

**Property to Be Searched
(SUBJECT TELEPHONE)**

This warrant applies to records and information associated with the cellular telephone assigned call number **(804) 433-8241**, with IMEI **357341090891638**, (“the Account”), that are stored at premises controlled by **T-Mobile** (“the Provider”), headquartered at **3625 132nd Ave SE, Bellevue, WA 98006**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account (**SUBJECT TELEPHONE**) listed in Attachment A for the time period **April 10, 2020 through December 20, 2020**:

- a. The following information about the customers or subscribers of the Account:
 - i. Names (including subscriber names, user names, and screen names);
 - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
 - iii. Local and long distance telephone connection records;
 - iv. All payment related information;
 - v. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
 - vi. Length of service (including start date) and types of service utilized;
 - vii. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);

- viii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
 - ix. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. The following historical stored telecommunications records associated with the SUBJECT ACCOUNT for the time period of **April 10, 2020 through December 20, 2020**:
 - i. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the SUBJECT ACCOUNT, including:
 - 1. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
 - 2. information regarding the cell towers and sectors through which the communications were sent and received.

II. Information to be Seized by the Government

All information described above in Section I that constitutes evidence, fruits, contraband, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2)(A), Receipt of Child Pornography involving DEON DOUGLAS, during the period of **April 10, 2020 through December 20, 2020**.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are

authorized to review the records produced by the PROVIDER in order to locate the things particularly described in this Warrant.